Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y teoría de Galois

Examen de Agosto (curso 2019)

1. Sean p, q números primos tales que $p < q$, y sea G un grupo de orden pq.

   a) Mostrar que $G \cong \mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$ para algún morfismo $\tau : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$, y que G es abeliano si y sólo si τ es trivial.

   b) (P 2 E 7) Probar que todo morfismo $\tau : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$, $\bar{k} \to \tau_{\bar{k}}$ es de la forma

   $$\tau_{\bar{k}}(n) \equiv r^k n \pmod q$$

   siendo $r \in \mathbb{Z}^+$ tal que $r^p \equiv 1 \pmod q$.
   (Recordar: como q es primo, por P2 E6 tenemos $\mathrm{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_q^*$).

   c) (P 3 E 11b) Probar que si $q \equiv 1 \pmod p$ entonces existe $r \in \mathbb{Z}$ tal que $r^p \equiv 1 \pmod q$ y $r \not\equiv 1 \pmod q$. Deducir que en este caso existen grupos no abelianos de orden pq.

   d) Probar que si $q \not\equiv 1 \pmod p$, entonces se tiene $G \cong \mathbb{Z}_{pq}$.

2. (P 7 E 5) Sea $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$ y $G = \mathrm{Gal}_{\mathbb{Q}}(f)$.

   a) Observando que f es irreducible, probar que $|G|$ es múltiplo de 5.

   b) Probar que f tiene 3 raices reales y dos imaginarias. Luego $\sigma \in G$, $\sigma(z) = \bar{z}$ define una transposición en el conjunto de raíces.

   c) Probar que $G \cong S_5$.

3. (P 6 E 13) Sean $f = X^4 + X^2 + 1 \in \mathbb{Q}[X]$ y $w = \frac{-1+\sqrt{3}i}{2}$. (Recordar que $w^3 = 1$).

   a) Probar que $\mathbb{Q}(w)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$ y calcular $[\mathbb{Q}(w) : \mathbb{Q}]$.

   b) Deducir que f es reducible en $\mathbb{Q}[X]$, y expresarlo como producto de irreducibles. Exhibir dos polinomios irreducibles distintos con el mismo cuerpo de descomposición.